



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/510,284	11/09/2005	Christophe Giraud	0579-1071	7544
466	7590	04/13/2009		
YOUNG & THOMPSON 209 Madison Street Suite 500 ALEXANDRIA, VA 22314			EXAMINER REVAK, CHRISTOPHER A	
			ART UNIT 2431	PAPER NUMBER
			MAIL DATE 04/13/2009	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/510,284	Applicant(s) GIRAUD, CHRISTOPHE	
	Examiner Christopher A. Revak	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06 October 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☒ Claim(s) 6 and 7 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 October 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>10/6/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on October 6, 2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
- (e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
- (f) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.

(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(g) BRIEF SUMMARY OF THE INVENTION.

(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).

(i) DETAILED DESCRIPTION OF THE INVENTION.

(j) CLAIM OR CLAIMS (commencing on a separate sheet).

(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

3. The disclosure is objected to because of the following informalities: It is noted by the examiner that the specification fails to include sections headers such as "Background of the Invention", "Brief Summary of the Invention", "Brief Description of the Drawings", and the "Detailed Description of the Invention".

Appropriate correction is required.

Claim Objections

4. Claim 6 and 7 are objected to because of the following informalities: Claim 6 recites "characterized in that is applied to a so-called AES algorithm that is known per se". The language of claim 6 appears indefinite indicating in some manner that it could be a literal translation. The examiner suggests amending the claim to recite "characterized in that is applied to an AES algorithm". Claim 7 recites of similar language. Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-8 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-7 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of *In Re Bilski* 88 USPQ2d 1385. The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The claimed method including steps of comparing round values against recalculated values to determine if they match which is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Art Unit: 2431

8. Claims 1-9 are rejected under 35 U.S.C. 112, first paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

A single means claim, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. In re Hyatt, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983) (A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only those means known to the inventor.). When claims depend on a recited property, a fact situation comparable to Hyatt is possible, where the claim covers every conceivable structure (means) for achieving the stated result while the specification discloses at most only those known to the inventor.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2431

10. Claims 1-5 and 7-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Callum, U.S. Patent 6,985,581.

As per claim 1, it is taught of a method of making an electronic entity with encrypted access secure when said electronic entity comprises means for executing a cryptographic algorithm consisting in applying to an input message a succession of groups of operations known as "rounds" involving a series of respective sub-keys ($K_{sub.0} \dots K_{sub.n}$) produced successively by an iterative process starting from an initial key K , which method is characterized in that it consists in storing a result of an intermediate step ($R_{sub.m}, K_{sub.n}$) of said iterative process, repeating at least some of the steps of said iterative process until a result is recalculated corresponding to the result that has been stored, comparing the value of said stored result to the value of the corresponding recalculated result, and prohibiting the broadcasting of an encrypted message (MC) resulting from the application of said algorithm if said two values are different (col. 1, line 66 through col. 2, line 13 and col. 4, line 23 through col. 5, line 9).

As per claim 2, it is disclosed of a method according to claim 1, characterized in that it consists in storing a sub-key ($K_{sub.n}$) and repeating at least some of the steps of said iterative process until a sub-key is recalculated corresponding to said stored sub-key (col. 4, line 23 through col. 5, line 9).

As per claim 3, it is taught of a method according to claim 1, characterized in that it consists in storing the value of an intermediate result ($R_{sub.m}$) of said iterative process and repeating at least a portion of said iterative process until an intermediate

result is recalculated corresponding to the stored intermediate result (col. 4, line 23 through col. 5, line 9).

As per claim 4, it is disclosed of a method according to claim 2, characterized in that it consists in storing the value of the final sub-key (K.sub.n) and repeating at least a final portion of the steps of producing the succession of said sub-keys until said final sub-key is calculated a second time (col. 4, line 23 through col. 5, line 9).

As per claim 5, it is taught of a method according to claim 4, characterized in that it consists in repeating all of the steps of producing the succession of said sub-keys (col. 4, line 23 through col. 5, line 9).

As per claim 7, it is taught of a method according to claim 1, characterized in that it is applied to a so-called DES algorithm that is known per se (col. 3, lines 45-52).

As per claim 8, it is disclosed of an autonomous electronic entity characterized in that it comprises means for implementing the method according to claim 1 (col. 1, line 66 through col. 2, line 13 and col. 4, line 23 through col. 5, line 9).

As per claim 9, it is taught of an electronic entity according to claim 8, characterized in that it takes the form of a microcircuit card (col. 1, line 66 through col. 2, line 13 and col. 4, line 23 through col. 5, line 9).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2431

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Callum, U.S. Patent 6,985,581.

As per claim 6, the teachings of Callum fail to disclose of the use of AES. The examiner hereby asserts that it would have been obvious to apply the use of AES to the teachings of Callum. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply an alternative means of encryption to the teachings of Callum so that the teachings were not limited to be used solely with the DES algorithm. According to the Supreme Court, the teaching, suggestion, or motivation test (TSM test) is one of a number of valid rationales that could be used to determine obviousness. It is not the only rationale that may be relied upon to support a conclusion of obviousness. (*KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (2007)). The claim would have been obvious because the substitution of one known element for another (AES algorithm for the DES algorithm) would have yielded predictable results to one of ordinary skill in the art at the time of the invention.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

Art Unit: 2431

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 517-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2431